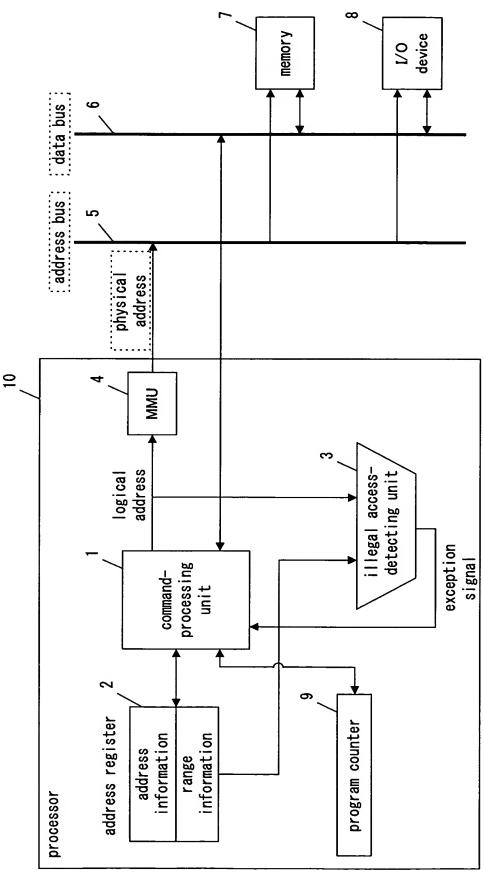
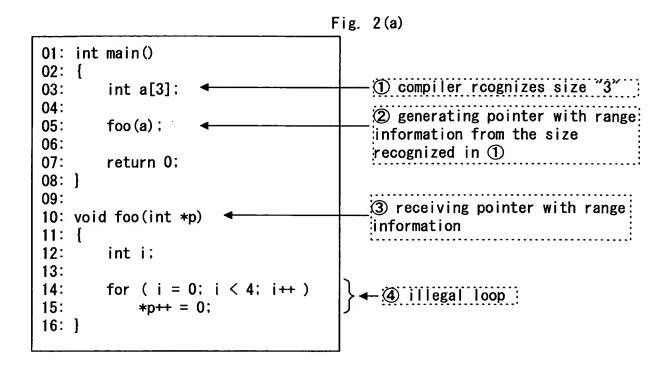
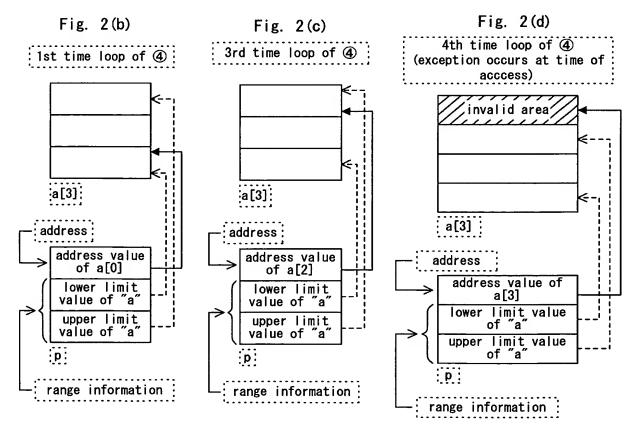
Fig. 1







## Fig. 3(a)

```
01: extern void input_str(char *str);
02:
03: int main()
04: {
05:
        char buf[32];
06:
        int len = 0;
07:
:80
        input_str(buf);
09:
10:
        while (buf[len] != 0)
11:
            len++;
12:
13:
        printf("%dThis is a character.\fomatsn", len);
14:
15:
        return 0;
16: }
```

## source code (main.c)

Fig. 3(b)

source code (input\_int.c)

Fig. 3(c)

failure recovering information file

Fig. 4(a)

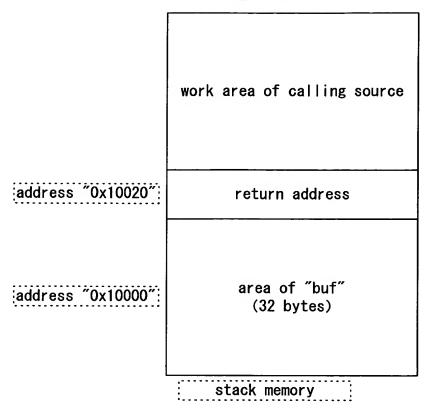


Fig. 4(b)

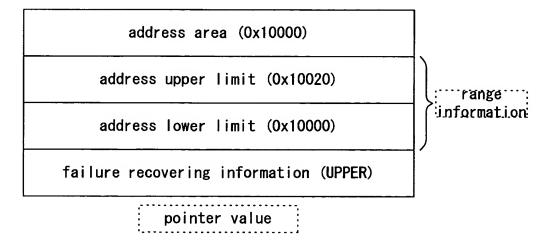


Fig. 5(a)

```
01: char a[5];
02:
03: extern void foo(char *p);
04:
05: int main()
06: {
07:     foo(&a[1]);
08:
09:     return 0;
10: }
```

Fig. 5(b)

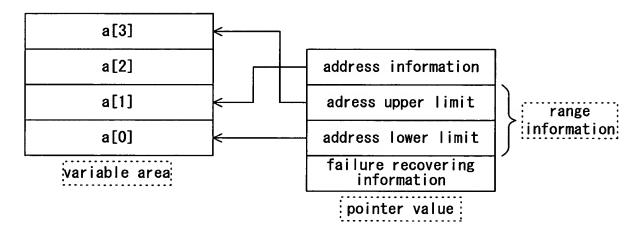


Fig. 6

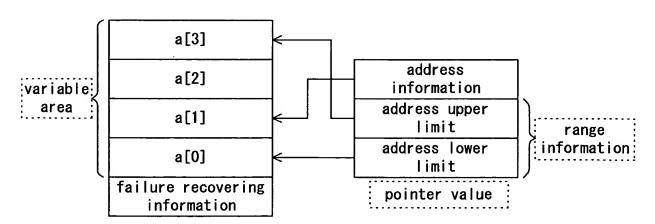


Fig. 7

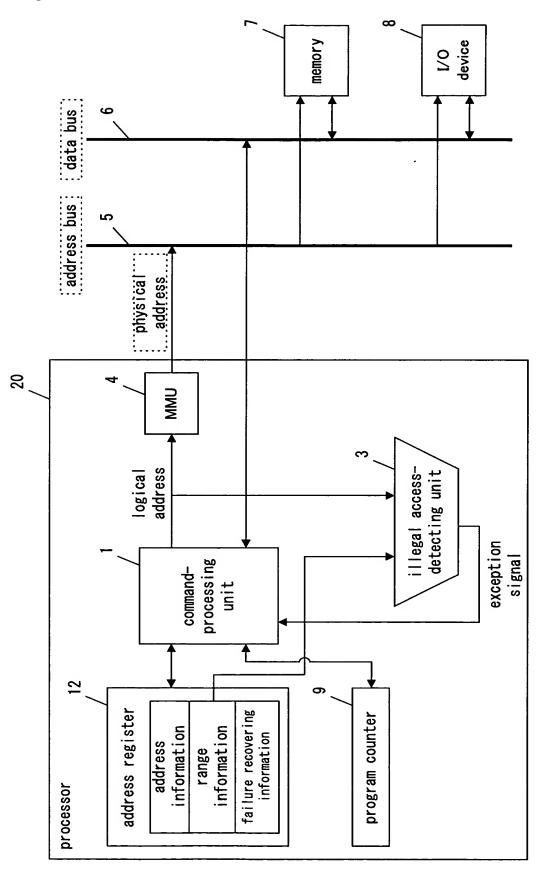


Fig. 8

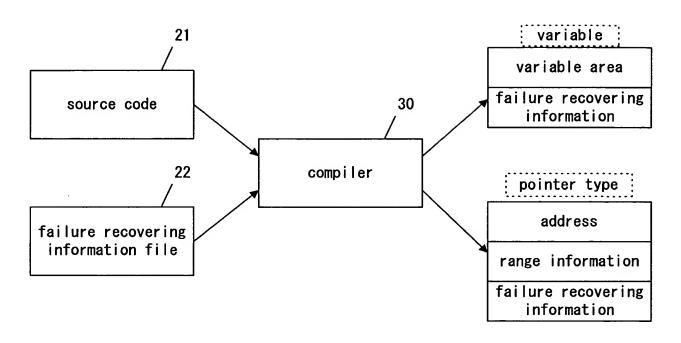


Fig. 9

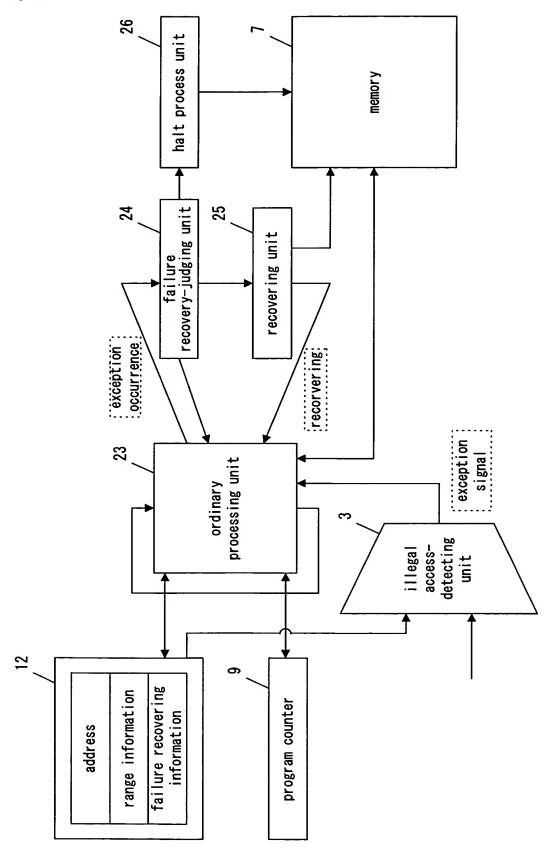


Fig. 10

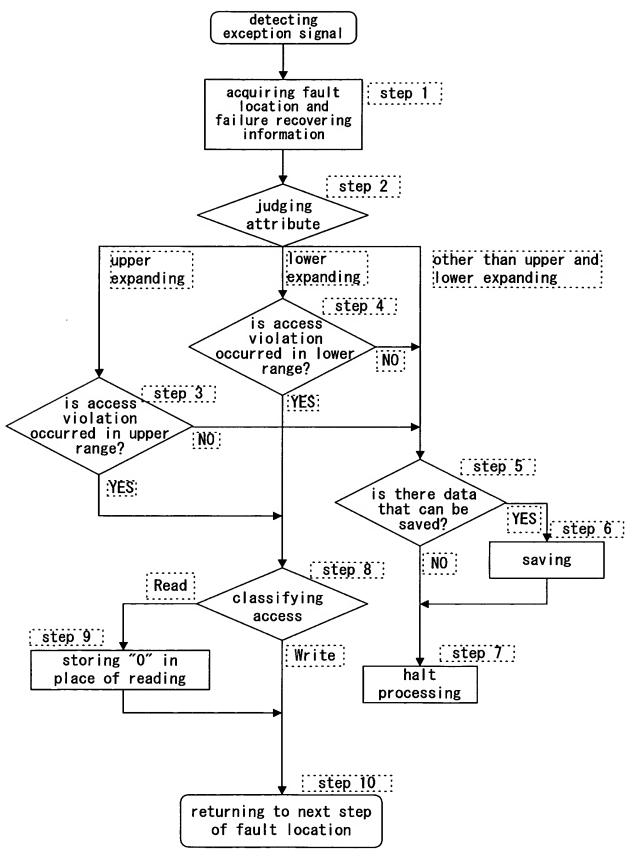


Fig. 11

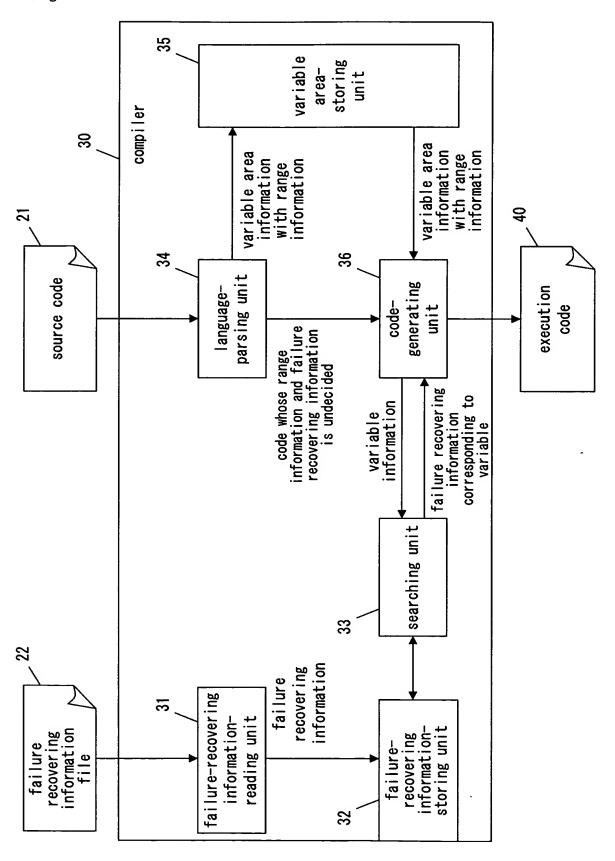


Fig. 12

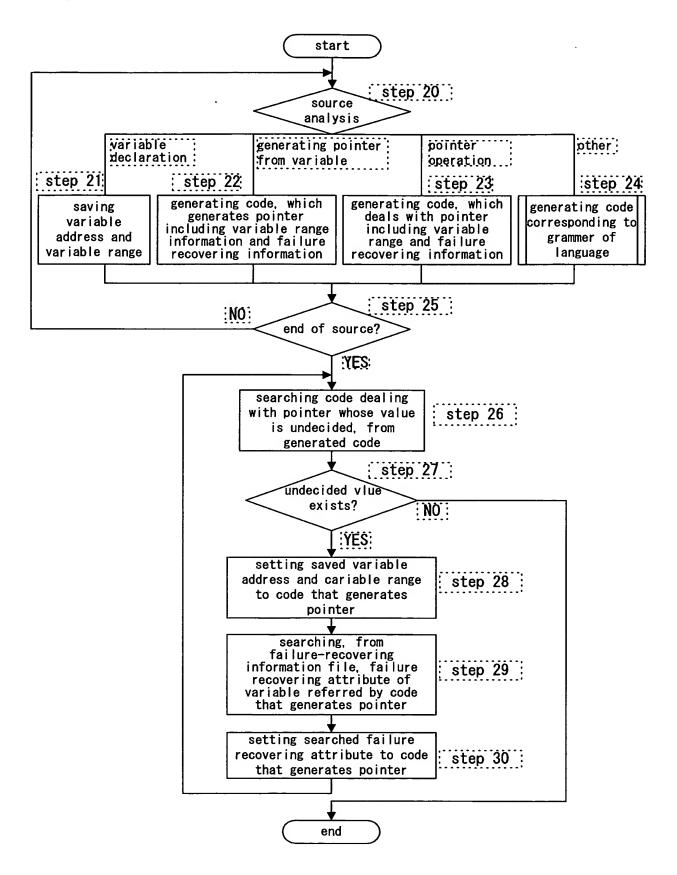


Fig. 13

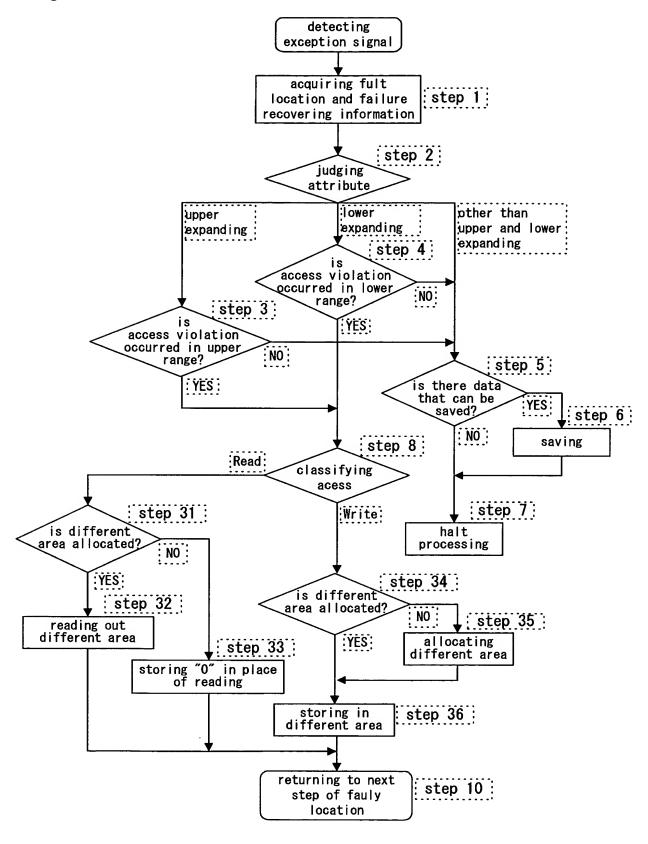


Fig. 14

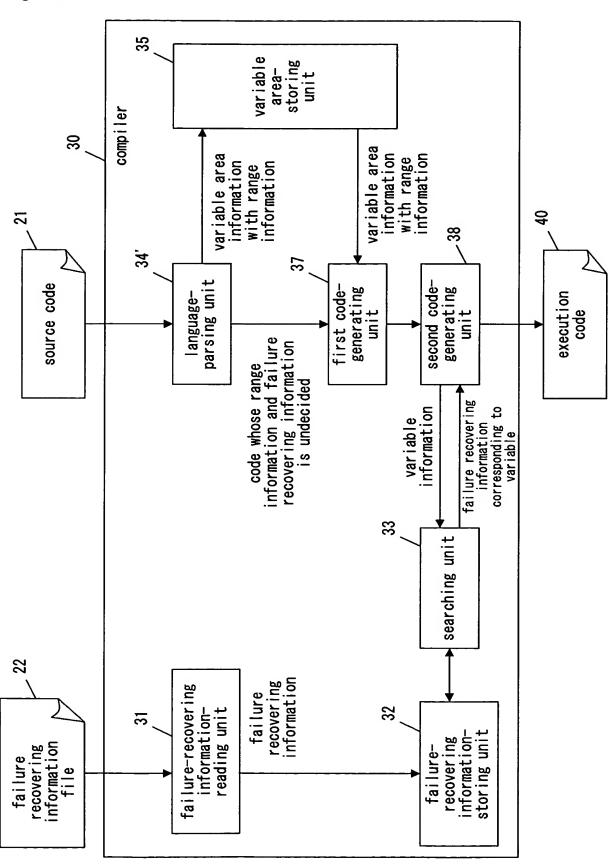


Fig. 15

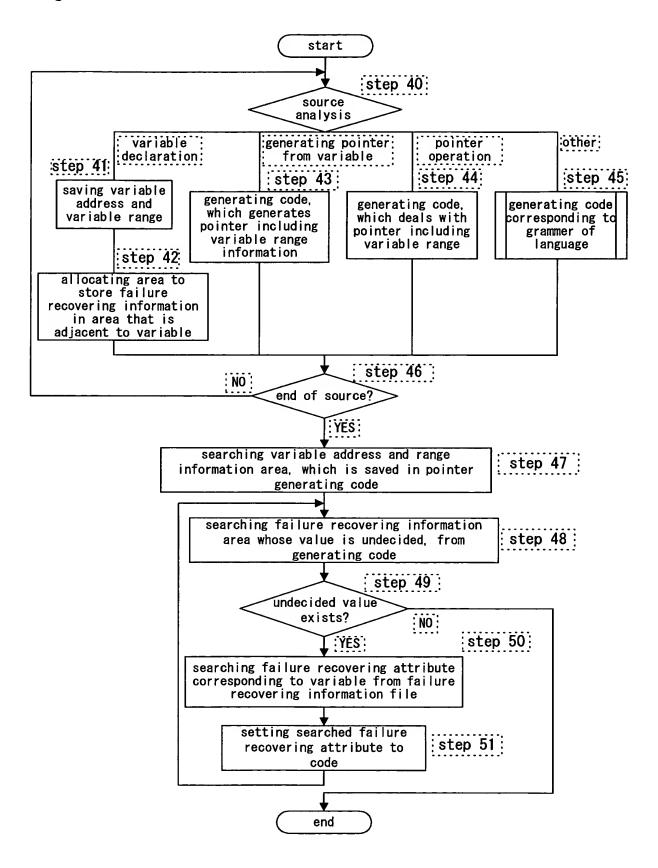


Fig. 16

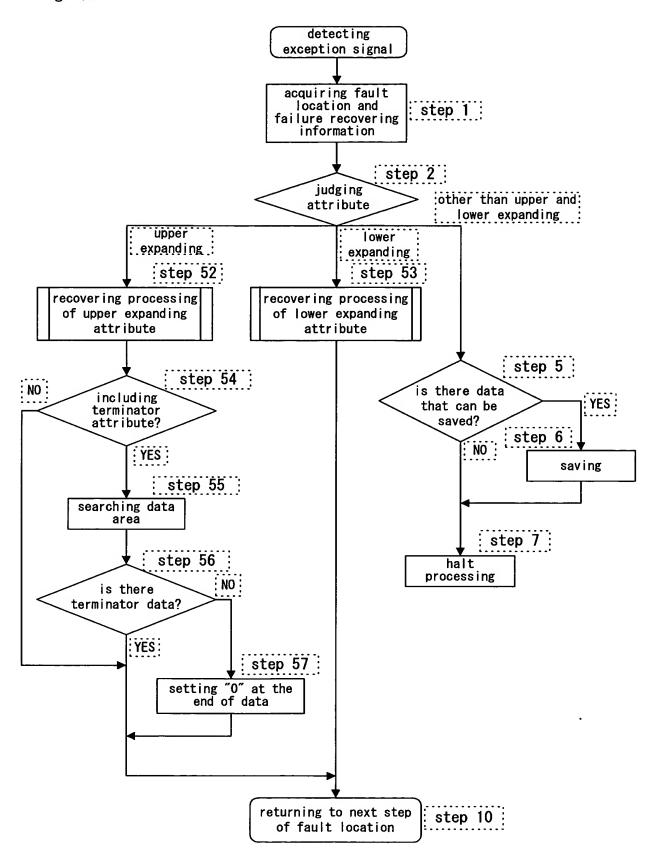
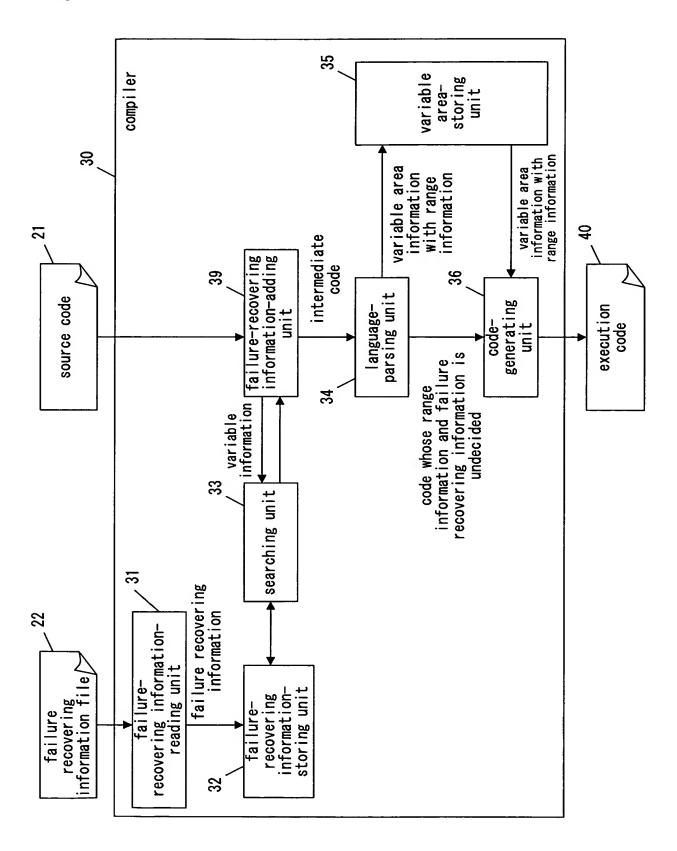


Fig. 17



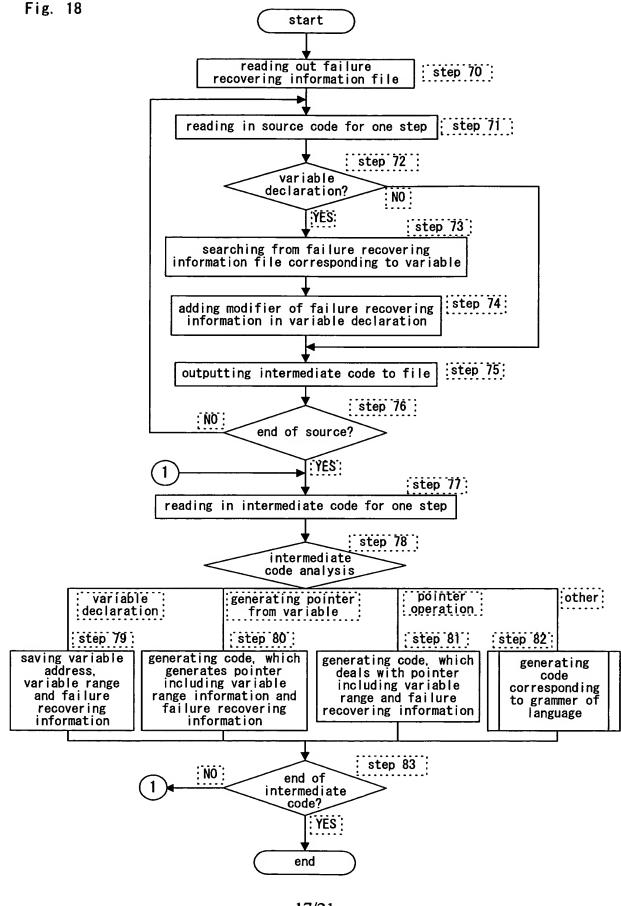


Fig. 19(a)

```
01: extern void input_str(char *str);
02:
03: int main()
04: {
05:
        UPPER char buf[32];
06:
       FIXED int len=0;
07:
08:
        input_str(buf):
09:
       while (buf[len] ! = 0)
10:
11:
            len++;
12:
13:
       printf("%dThis is a character¥n",
len);
14:
15:
       return 0;
16: }
         intermediate code
```

(after processing of "main, c)

## Fig. 19(b)

```
01: void input_str(char *str);
02: {
03:
          FIXED int c:
04:
05:
          while (c = getchar) ! = EOF
06:
              *str++=c;
07: }
```

intermediate code (input\_int.c);

Fig. 20

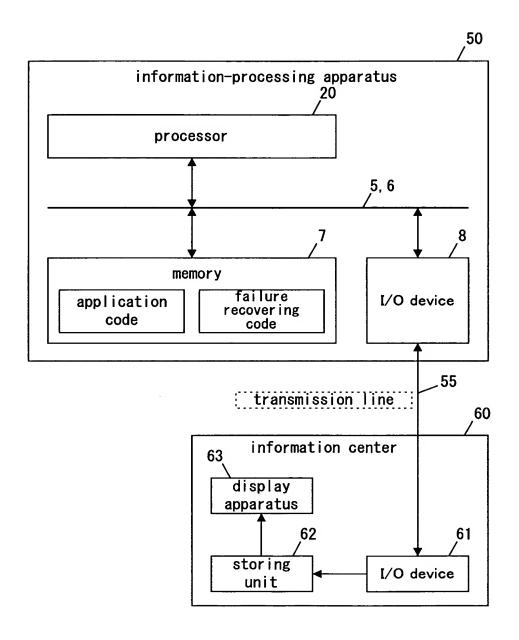


Fig. 21

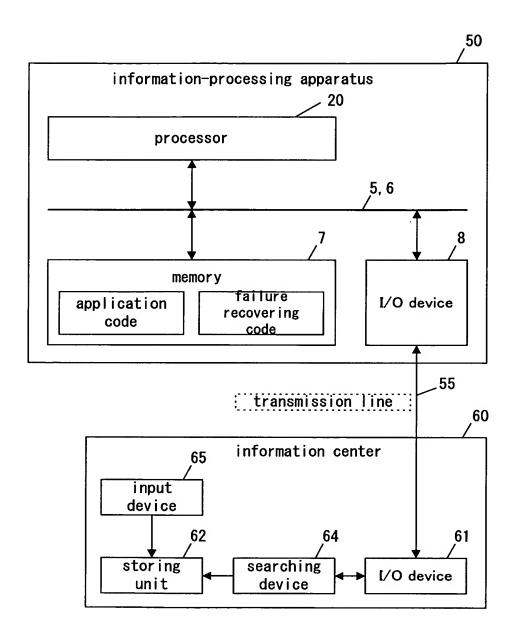


Fig. 22(a)

```
extern void read_str(char *str);
int read_int()
{
    char buf[32];
    read_str(buf);
    return atoi(buf);
}
```

Fig. 22(b)

work area of calling source

area of "buf" (32 bytes)

stack memory

Fig. 22(c)

attack code

address of attack code

dummy 32 bytes

data for attack